AMENDMENTS TO THE SPECIFICATION

Please amend the Title on page 1 as follows:

TAG PRIVACY PROTECTION METHOD, TAG DEVICE, BACKEND APPARATUS, UPDATER, UPDATE SOLICITOR~~, PROGRAMS THEREFOR~~ AND RECORD MEDIUM CARRYING SUCH PROGRAMS IN STORAGE

Please replace the paragraph beginning at page 2, line 14, to page 3, line 4 with the following amended paragraph:

[0004] [Issues in basic automatic tag identification system]

However, in the basic automatic tag identification system, anyone who is in possession of a reader can read tag ID information, and accordingly, there has been a risk that information of articles under control may leak through eavesdropped tag ID information.

As regards this, non-patent literature 2 (Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, Daniel W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," First International Conference on Security in Pervasive Computing.) discloses a method in which a tag device delivers a hash value to a reader.

According to this method, the tag device initially transmits a hash value H(id | r) for a bit combination of ID information id and a random number r to the reader, which sends them to the backend apparatus. The backend apparatus forms a bit combination of the received random number r and each id' stored in the database, and determines its hash value H(id' | r). Then it verifies whether or not the determined hash value H(id' | r) matches with the received hash value H(id | r), and transmits products distribution information or the like which corresponds to the matched id' to the reader. In this manner, a leakage of the tag ID

information to a third party can be prevented. It is to be noted that $H(*)$ means a processing which applies a hash function H to $*$.

Please replace the paragraph beginning at page 3, lines 5-20 with the following amended paragraph:

[0005] In a method disclosed in Japanese Patent Applications No. 2003-111342 and No. 2003-113798 which are not yet made open, a privileged ID which makes tag ID information confidential is employed to prevent a leakage of tag ID information to a third party. Specifically, in these techniques, a privileged ID is stored in a tag device, and a client apparatus which has read the privileged ID solicits a security server apparatus on a network to decrypt the privileged ID. In response to the solicitation, the security server apparatus responds with a plain text tag ID information which is a decrypted result for the privileged ID after it has confirmed that the client is a regular client apparatus. In this manner, a leakage of tag ID information to a third party can be prevented.

non-patent literature 1: EPC global, Inc., "EPC global", [online], [retrieved September 9, 2004]~~, internet <http://www.epcglobalinc.org/>~~.

non-patent literature 2: Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, Daniel W. Engels, Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, First International Conference on Security in Pervasive Computing.

Please replace the paragraph beginning at page 4, lines 17-25 with the following amended paragraph:

[0007] Also in the method disclosed in Japanese Patent Application No. 2003-111342 or the like, for example, because the radio tag device always returns a same privileged ID, the attacker can trace the distribution process of the tag device by tracing the privileged ID if he cannot decrypt ID in plain text.

The present invention has been made in view of such aspect, and has for its object the provision of a technology which is capable of preventing a tracing of the distribution process of tag device by a third party.

MEANS TO SOLVE ~~ISSES~~ISSUES

Please amend the Abstract of the Disclosure on page 175 of Applicants' specification as on the following page: